Activate the Dynamic Delegation Process in X.509 Certification via a New Extension

MOUTASEM SHAFA'AMRY
Faculty of Informatics Engineering
Arab International University (AIU)
Daraa -Damascus Highway, Daraa, Syria
SYRIA
Email: m-shafaamry@aeu.ac.sy, web address: www. aeu.ac.sy

NISREEN ALAM ALDEEN
Department of Informatics, Faculty of Sciences
Damascus University
SYRIA
Email: miss_nisreen2000@yahoo.com

Abstract: The increasing number of clients and users of e-banking, e-government and e-application through digital communications, made it a must to develop new methods and solutions for authentications and secure access. Digital certificates are one of these methods for secure transactions, X.509 certificate is one standard for these digital certificates, Despite the fact that x.509 certificate is of high level of security and authenticity, it has many weaknesses as not applying dynamic delegation to it.. The efficiency of proxy certificate which proposed as a practical solution in the field of dynamic delegation could not find solutions for its weaknesses Which were the main motivation to work on this research trying to come up with new solution which integrates the pros of X.509 and the pros of Proxy certificate to benefit from the specifications of each one and to avoid the weaknesses of them. this paper will cover the standard of Digital certificates and its relation with dynamic delegation, focusing on the weaknesses of applying these standards to dynamic delegation then we propose our solution to make it applicable and more efficient to apply dynamic delegation to digital certificate standards. Finally we will cover the pros and cons of our new solution, some conclusions and future work.

Key-words: Digital certification systems, X.509 standard, Proxy Certificates, authentication (PCA), Dynamic delegation, Identity verification, Network security, e-security

1. Introduction

The Increase of e- applications using digital networks to exchange sensitive data has created a need for greater confidence in the identities of the parties involved in the communication. digital certificates, which are a sort of online passport links between the user and his public/private keys, provide a supported level of authentication and privacy to digital communications that cannot be achieved by passwords alone. Different standards of digital certificates are developed, each one based on its own framework architecture, and has advantages and disadvantages.

No doubt that the establishment of X.509 public key certificates [7], which is the earliest framework to provide and support authentication has its great implementation features, as it provides a sufficient authentication infrastructure for entities. However, x.509 has various limitations, such as the lake of delegation [11]. This is one of the requirements motivated the development of Proxy Certificates. Proxy Certificates which have been refined through standardization in the IETF PKIX working group [6] and have achieved RFC status (RFC3820), allow an entity holding a standard X.509 public key certificate to delegate some or all of its privileges to another entity which may not hold X.509 certificates. This delegation can be performed dynamically without the intervention of a third party. Proxy Certificates can be integrated with different types of authorization systems, However they have been suffering from problems. And as it happens the belief that ideal solution had been achieved was wrong, and the race has been on to build an ideal and reliable certification structure. We provide in this paper our suggested solution to improve the process of delegations that overcome the proxy certification problems.

2. Dynamic delegation principle:

Dynamic delegation is a state when user A wants to grant his rights (or a part of his rights) to user B to access his resources and applications for predefined period of time and without any reference to the roots.

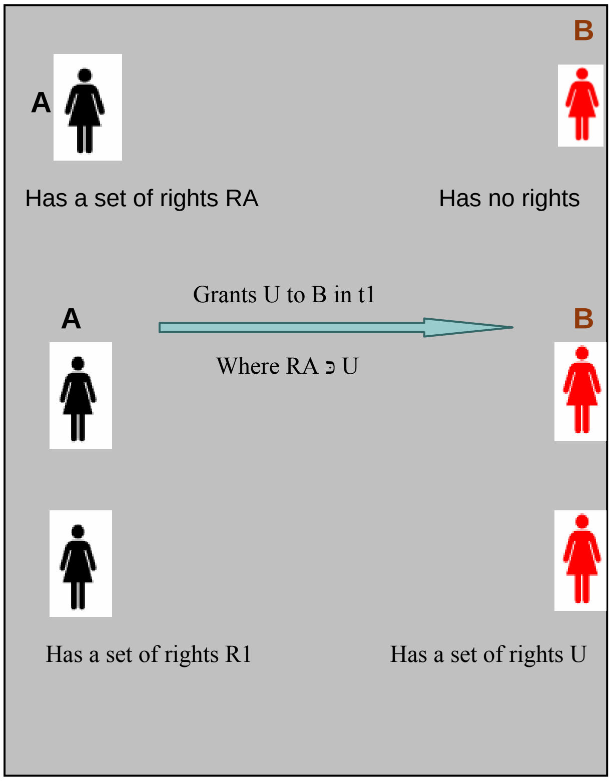


Figure.1: delegation principle

3. X.509 and Dynamic delegation

X.509 [1] is the ITU standard for the public key based authentication framework. It was invented in 1988; later on newer version of it comes to life (figure.2).

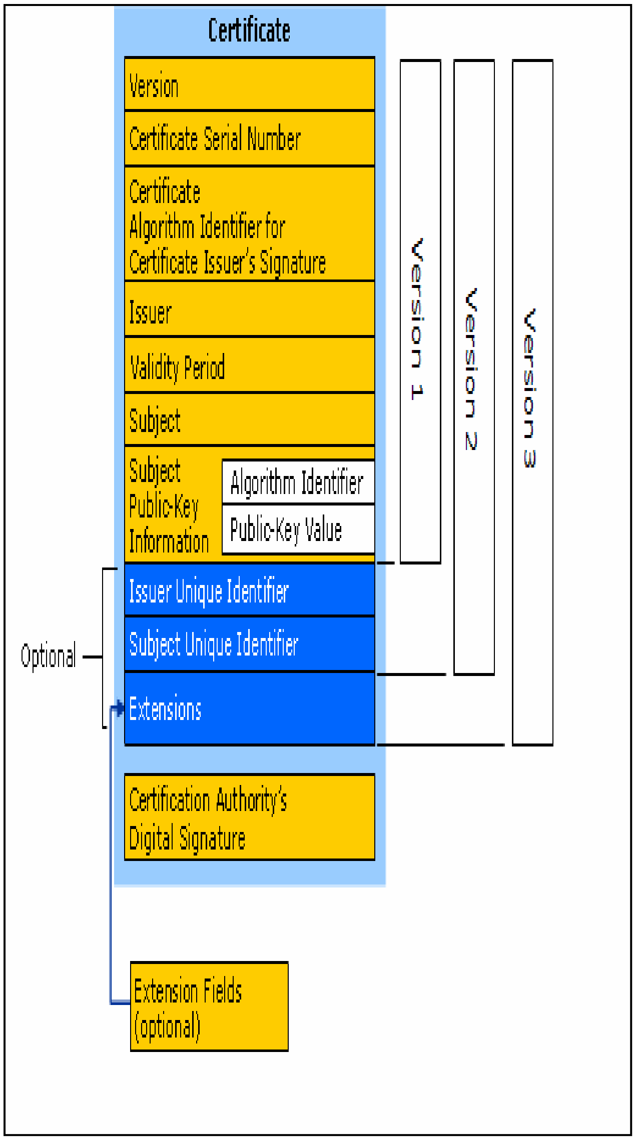

Certificate
Version
Certificate Serial Number
Certificate Algorithm Identifier for Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject Public-Key Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature
Optional
Extension Fields (optional)
Version 1
Version 2
Version 3

Figure.2: the general structure for x.509 standard certificate

The public key infrastructure of this standard is hierarchical (as shown in figure.2).

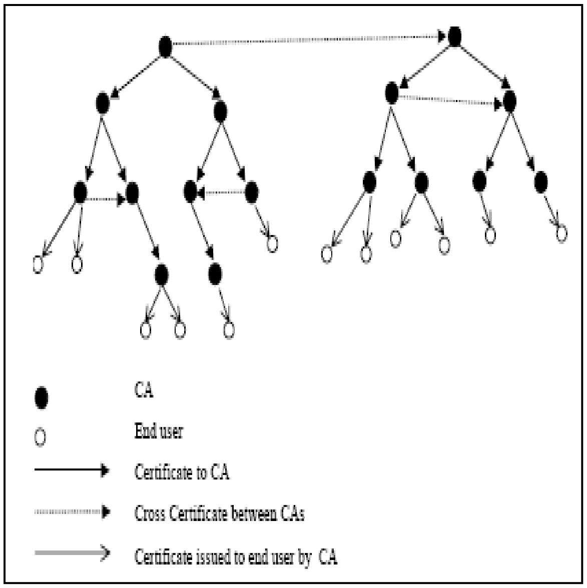

CA
End user
Certificate to CA
Cross Certificate between CAs
Certificate issued to end user by CA

Figure.3: Typical X.509 Based PKI (Levi, 1999)

The certificate structure in X.509 is basically the guarantee of the binding between the identity and the public key of an entity. The certificates are issued by commonly known and trusted Certification Authorities (CAs). X.509 is part of the X.500 series of recommendations that define a directory service [2]. The directory is a distributed set of servers that maintains a database of information about users. In X.509, the directory serves as a store of classical certificates.

X.509 is good for encrypted transactions (e.g. between browser and server), and a strict hierarchy is required, as it is considered the most suitable choice when we need to raise confidence in transactions.

However, truly several cases exist that are not well covered by X.509 public key certificates alone [11] such as:

- **delegation:** It is the case in which user needs to delegate some subset of their privileges to another entity for a brief amount of time.
- **Dynamic entities**: In addition to delegation to services and entities, the requirement exists to support delegation of privileges to services that are created dynamically, often by the user himself, that do not hold any form of identity credential.
- **Repeated Authentication**: It is common process to protect the private keys associated with X.509 public key certificates either by encrypting them with a pass or by requiring a PIN for access. This technique costs a heavy load on users who need to authenticate repeatedly in a short period of time.

4. Proxy certificate:

4.1. The Need for Proxy Certificates

As we can see from the above description of the X.509 certification, applying dynamic delegation to X.509 is not applicable because of the resulted load and complicated process when dealing with the hierarchical environments

This requirement was one of the essential factors which led to develop the X.509 Proxy Certificate, as an authentication solution allows users to create identities for new entities dynamically in a light-weight manner, without any intervention from CAs. the first prototype of Proxy certificate was proposed to meet the requirements of GSI (Grid Security Infrastructure), later on proxy certificate has been used to build many of middleware libraries and applications [4].

Recently, the ability and efficiency of using proxy certificates in the field of mobile agent technologies, to facilitate security for mobile agents, have been proved [9].

4.2. Issuing a Proxy Certificate

Proxy Certificate is a standard mechanism for dynamic delegation and identity creation in public key infrastructures, based on X.509 public key Certificates. Unlike a public key certificate, the issuer (signer) of a Proxy Certificate is identified by a public key certificate or another Proxy Certificate instead of a Certification Authority (CA).

Proxy Certificates use the same format of X.509 public key certificates [3],[5], and serve to bind a unique public key to a subject name, as a public key certificate does.

Proxy Certificates have three obvious modes of integration with authorization systems:

- Full delegation of rights to the Proxy Certificate bearer.
- No delegation of rights only using attribute assertions to grant privileges.
- Restricted delegation of some of the issuer's rights to the Proxy Certificate bearer.

The Proxy Certificate RFC defines two policy methods that must be understood by all implementations of Proxy Certificates:

- Proxying: the issuer of the Proxy Certificate intended to delegate all of their privileges to the Proxy Certificate bearer.
- Independent: the issuer of the Proxy Certificate intended the Proxy Certificate by itself to convey none of the issuer's privileges to the bearer. In this case the Proxy Certificate only serves to provide the bearer with a unique identifier.

For both of these methods, the policy field is empty, since the intended delegation policy is explicit in the type.

4.3. Proxy Certificate Contents

Actually both X.509 public key certificate and Proxy Certificate have similar contents (as shown in figure.4), except some essential differences:

- The subject name of a Proxy Certificate is scoped by the subject name of its issuer to achieve uniqueness. This is done by appending a CommonName Relative Distinguished Name component (RDN) to the issuer's subject name.
- The value of the serial number and the added CommonName RDN should be statistically unique to the issuer and to it's scope. Uniqueness for both of these values is achieved by using the hash of the public key as the value.
- The public key in a Proxy Certificate is distinct from the public key of its issuer and may have different properties. Except when using Proxy Certificates for single sign-on, the issuer does not generate the public key-pair and has no access to the private key.
- Proxy Certificate must bear a newly-defined X.509 extension, the Proxy Certificate Information (PCI) extension. The PCI extension essentially contains the following fields:
  - Policy Method Identifier: it is an object identifier (OID) that identifies the delegation policy method used in the policy field.
  - Policy Field: contains an expression of the delegation policy that has a format specific to the particular method (and may be empty for methods that do not require additional policy)
  - The PCI extension also contains a field expressing the maximum path lengths of Proxy Certificates that can be issued by the Proxy Certificate in question.

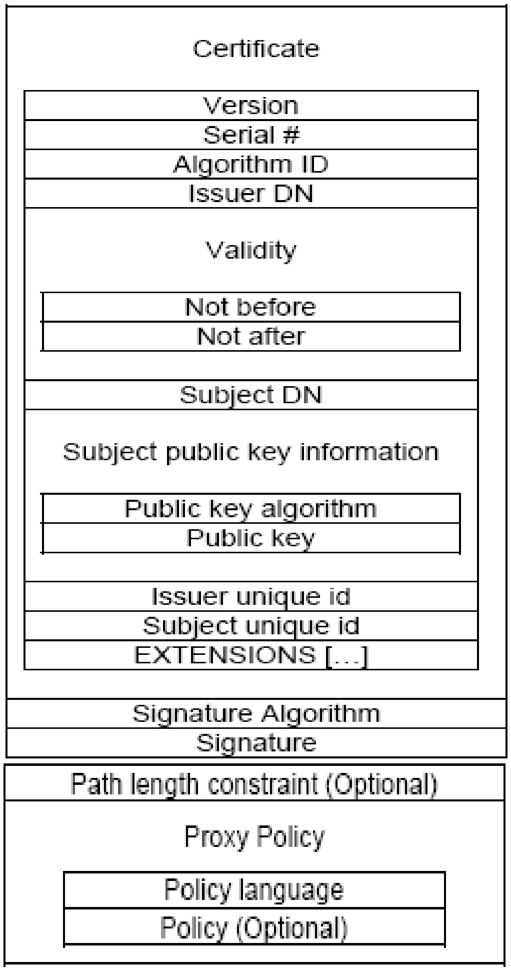


Figure.4: Structure of a proxy certificate (John Gilbert, Russell Perry, 2008)

4.4. Management of Proxy Certificate

Due to the fact that the Proxy Certificate is identified by a public key certificate, or another Proxy Certificate rather than a certification authority (CA), therefore, a proxy certificate can be created dynamically without requiring the heavy-weight process associated with obtaining public key certificates from a CA.

The public key in a Proxy Certificate is distinct from the public key of its issuer, and may have different properties except when using Proxy Certificates for single sign-on.

Proxy Certificate is used by its bearer to authenticate and establish secure connections in the same manner as a normal X.509 end-entity certificate, so it preserves the characteristics of standard X.509 based PKI (PKIX).

Validation of a certificate chain has many rules, as it's described by RFC 3280 [5] and Proxy Certificate RFC [10]. These rules are:

- Ensuring each Proxy Certificate has a valid Proxy Certificate Information extension.
- Each Proxy Certificate must have a subject name derived from the subject name of its issuer.
- Verifying the number of Proxy Certificates in the chain does not exceed the maximum length specified in any of the Proxy Certificate Information extensions in the chain.
- Storing the delegation policies of each Proxy Certificate, so that the end party can determine the set of rights delegated to the bearer of the end Proxy Certificate used to authenticate.

4.5. Evaluation of Proxy Certificates:

The current standard of Proxy certificate has some advantages and disadvantages. We will summarize them in the following points:

4.5.1. Advantages

The main advantages of the proxy certificates are:

- Use of the same format as X.509 public key certificates allows Proxy Certificates to be used in protocols and libraries in many places as if they were normal X.509 public key certificates which significantly eases the implementation.
- Proxy Certificates can be used to perform single sign-on and Lightweight Mutual Authentication [12]
- Proxy Certificates can be created to delegate privileges from an issuer to another party over a network connection without exchanging the private keys.

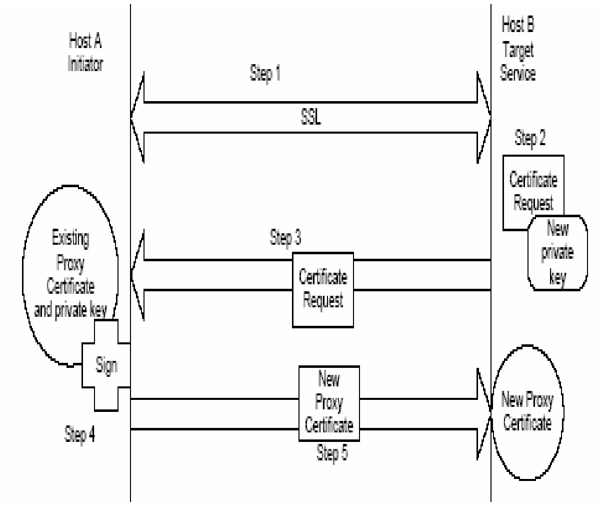


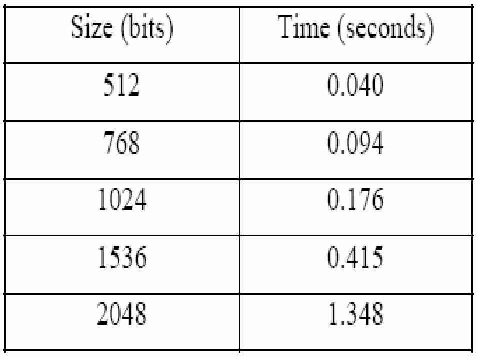
Figure.5: Delegation mechanism (Von Welch2005)

4.5.2. Disadvantages

The main disadvantages of the proxy certificates are:

- The Proxy Certificate private key is stored on a local file system and is protected by only local file system permissions.
- Generating a new key pair involves finding a pair of suitable prime numbers (which is a non-trivial amount of work), is the expensive part of a Proxy Certificate creation. Furthermore, scales exponentially with the key length. Note that Proxy Certificate generation comes with a non-negligible penalty in server-side key generation [11].

Table1 shows timings for RSA key pair generation on a 2.8GHz Pentium 4 processor using the OpenSSL 0.9.7 library [11].



Size (bits)	Time (seconds)
512	0.040
768	0.094
1024	0.176
1536	0.415
2048	1.348

Table1: Key generation times for RSA key pairs
(X.509 Proxy Certificates for Dynamic Delegation, 2005)

- Lack of define a special delegation language or modify the various applications to be able to understand the existing languages.
- The form of Proxy Certificates with Restricted Delegation tends to be difficult and, in this case, the implementation becomes more complex, due to that Proxy Certificates do not mandate any particular delegation language for the issuer to express their delegation policy. Without assurance that the application will handle the enforcement of the restrictions, the authentication library cannot safely accept a restricted Proxy Certificate. For this reason, this form of Proxy Certificate authorization isn't used to a large degree.
- There is no implemented method for revocation of proxy Certificates, maybe the short lifetime limits the length of misuse if a Proxy Certificate were to be compromised, but it could be a real problem when a value of zero was not involved in a field expressing the maximum path lengths of Proxy Certificates. In this case the length of the path is unlimited. A kind of revocation mechanism for proxy certificates to improve the security and availability of grid computing was presented [8].

  This solution is based on the existing Public Key infrastructure (PKI), with additional trusted third party named the Certificate Register Authority (CRA) which has the following main tasks:
  - Maintain delegation relations of PCs for grid clients
  - Supplying detailed information about PCs and the delegation information (by request)
  - Generate PCTL (proxy certificate trust list) which suggested to record trusted delegation traces for grid computing.
  - Revoke fishy or expired PCs.

  The proposed PCTL (proxy certificate trust list) which is signed by CRA, records PCs information that are involved in the delegation process.

  The format for each entry in PCTL depends on different levels of security due to the included certificate information:
  - High Security Level
  - Middle Security Level
  - Low Security Level

  Despite the fact that the proposed solution enhanced the level of authenticity, but it tried to solve the revocation partially for specific application as grid computing, as it has many disadvantages:
  - This method tried to benefit from the specifications of hierarchical structures without avoiding the weaknesses of these environments, so an additional resulted load and complicated process to the delegation operation need to be considered.
  - additional overhead of the this solution is the Additional negotiation and handshake between the issuer and CRA in the register phrase.
  - bottle-neck and single-point failure problems need to be considered To support PCTL,

However, this method could not achieve a dynamic delegation changes which are the original purpose of proxy certificate

These points of proxy certification disadvantages are the motivation of our research currently working on. We concentrate on improving the delegation process to overcome the following disadvantages of the current proxy certification system: the weakness of storing private keys, the complexity of generating pair of the keys.

As we can see from the above description of the proxy certification, Proxy Certificate is identified by a public key certificate or another Proxy Certificate rather than a certification authority (CA), In other words, the authority of providing the delegation is the entity himself, who has a certificate generated by X.509 Certificate Authority, or a delegated entity. The weak points are coming from the fact, that this entity is not qualified enough to have a complex structure for securing the private keys, or generating pair of keys. Therefore, our idea is simplifying the process of delegation with improvements to the current weak points available in the current scenario of Proxy Certification. We note that our scenario is still under process and not finalized yet.

5. The Proposed Solution:

5.1 The main idea:

Our idea depends on mixing a centralized strict hierarchical structure with stand-alone structure (the central and non-central structures) in order to make use of merits of both of these methods, and getting rid of point of weakness inherited in both of them.

We suggest in our method, adding a special annex to the original structure of the X.509 standard certification (figure.6) for the delegation propose. Therefore, we can use the public and private long-term keys in the operation of delegation without the need of generating new keys related to proxy operation.

5.2 Structure of the suggested annex

The suggested annex (as shown in figure.6) contains the following inactivated fields:

- A Field concerning the public key of the X.509 certificate related to the beneficiary (the person granting the proxy).
- A field special for the public key of the X.509 certificate related to the person granted the delegation.
- Special fields concerning the policy of the desirable proxy (similar to the fields found in PCI proxy certificate except the field that determines the maximum number of certificates), and these fields as follow:
    - policy method identifier field: The policy method identifier serves to identify the delegation policy method used in the policy field.
    - policy field: The policy field expresses the required policy of the delegation due to the desire of the beneficiary.
- A field of a pre-determined value which represents the time for the proxy (it is recommended to be relatively short such as eight hours).

Notice that the field expressing the maximum path lengths of Proxy Certificates that can be issued by the Proxy Certificate in question is not available due to the fact that our solution limits Delegating to one level of path.

Upon issue of the standard X.509 certificate, the center applies its seal (its electronic signature) only on the main part of the X.509 certificate, without signing the annex of delegation. The special annex of delegation should be signed by the beneficiary when he wishes to grand some or all of his privileges without referring to the authority certificate center which issued this certificate.

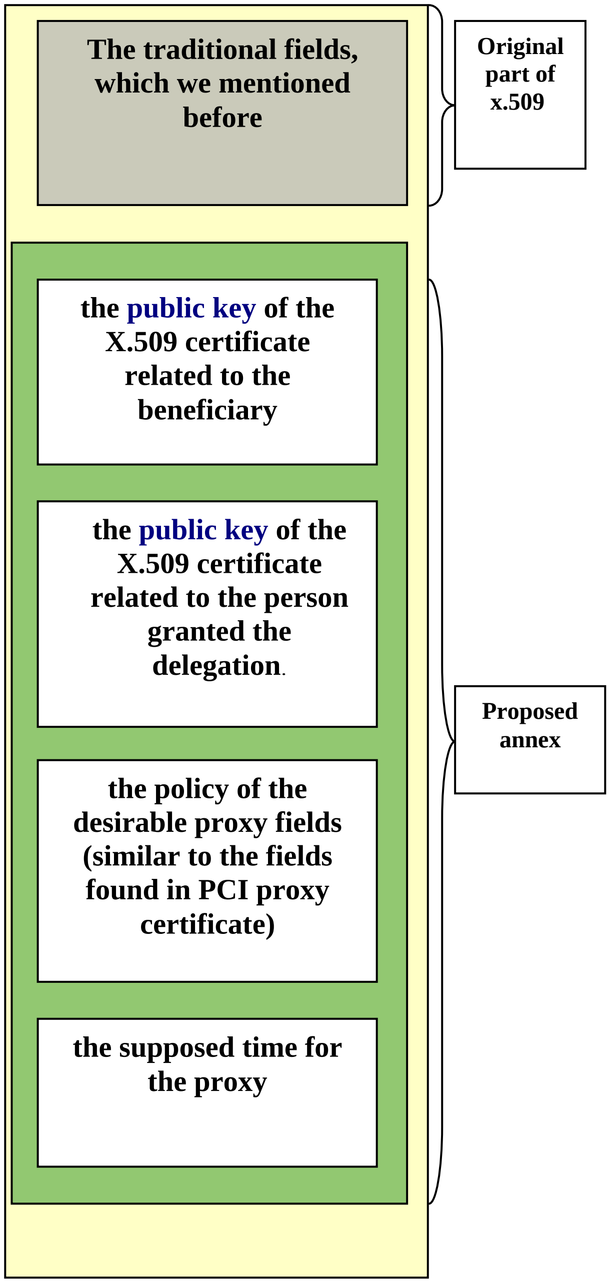

The traditional fields, which we mentioned before
Original part of x.509
the public key of the X.509 certificate related to the beneficiary
the public key of the X.509 certificate related to the person granted the delegation.
the policy of the desirable proxy fields (similar to the fields found in PCI proxy certificate)
the supposed time for the proxy
Proposed annex

Figure.6: the essential fields of suggested annex

5.3 Work Mechanism

When a holder of standard X.509 certificate wishes to delegate his rights (or some of them) to another user, the procedure will take the following steps explained in figure n:

- The first step: The beneficiary sends a proxy request to the person who intends to grant him this proxy.
- The second step: On the acceptance of the request, a secure channel between the client and the delegate is established using either SSL or TLS protocol.
- The third step: The person who gets the proxy then sends his certificate (the standard X.509 certificate) to the beneficiary through a secure communication channel.
- The forth step: The beneficiary fills the fields of the annex in the received certificate according to his needs (defining the required policy of proxy granting).
- The fifth step: the beneficiary signs the annex of the delegated certificate using his private key (the private key related to his X.509 certificate).
- The sixth step: the beneficiary sends back the certificate with his special signature on annex of the delegation.

The result is that the person who granted the delegation has his own X.509 certificate with a proxy annex signed by the beneficiary only without the need to the CA signature or reference.

When the person granted the proxy wants to enter one of the target's applications instead of the beneficiary, the intended application will do the following.

- First of all, he verifies the public key of the certificate as usual (verification of the basic part of X.509 certificate).
- When the public key of the delegate (in the standard part of X.509 certificate) is not authorized for this application, the application, then checks and verifies the annex of the certificate.

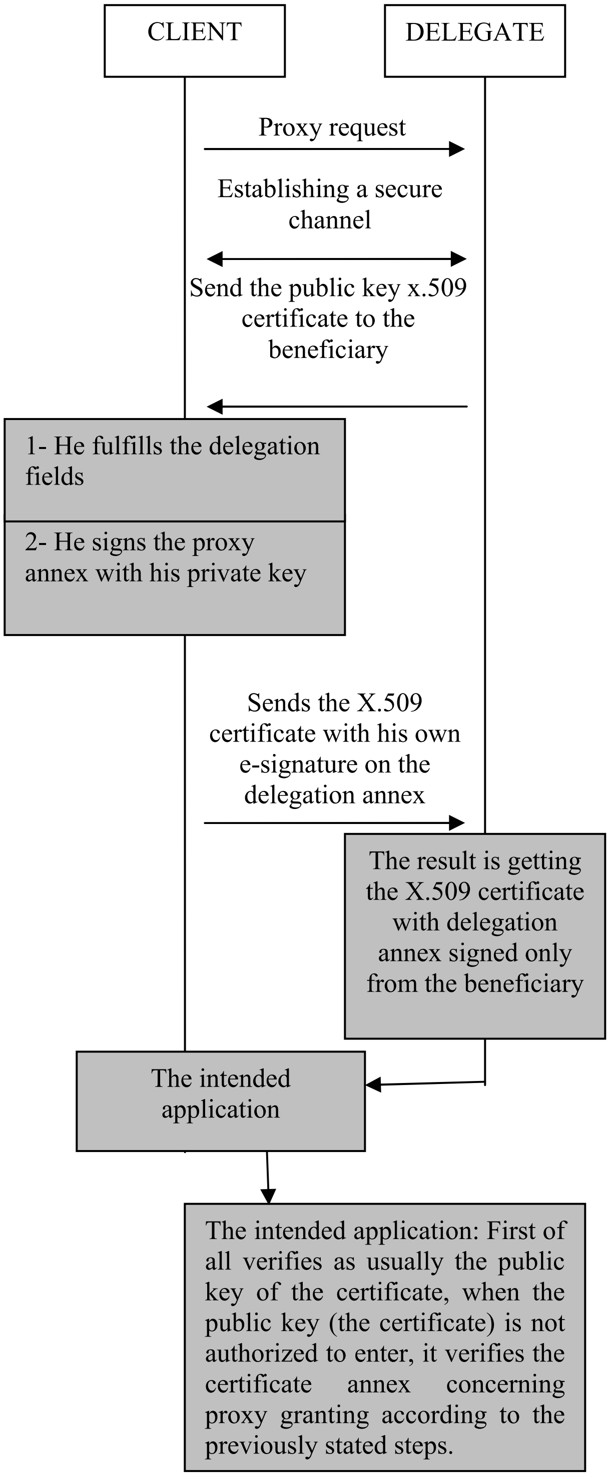

CLIENT
DELEGATE
Proxy request
Establishing a secure channel
Send the public key x.509 certificate to the beneficiary
1- He fulfills the delegation fields
2- He signs the proxy annex with his private key
Sends the X.509 certificate with his own e-signature on the delegation annex
The result is getting the X.509 certificate with delegation annex signed only from the beneficiary
The intended application
The intended application: First of all verifies as usually the public key of the certificate, when the public key (the certificate) is not authorized to enter, it verifies the certificate annex concerning proxy granting according to the previously stated steps.

Figure.7: Work Mechanism

5.4 Advantages of the suggested solution:

In this suggested method which is based on merging of X.509 certificate and proxy certificate we aim to exploit the high level of security in X.509, and avoiding the problems of hierarchical structure at the same time

Then getting the following features:

- No need to refer to the CA center to activate the operation of the proxy granting. It can be managed by only users who have certificates issued by the CA. Therefore, we gaining the advantages of the hierarchical structure in confidentiality and authentication without performing complex procedures required in those hierarchical structures.
- Reducing the time and memory consumptions of generating dedicated proxy certificates. As a dedicated proxy certificate usually has short life-time, and may need for many proxy certificates to generate.
- The choice of a time period which is previously defined for proxy granting makes the delegation to be canceled automatically after the expiration of the specified period. Therefore, there is no need to cancel the delegation. But, we planning for the future to deign a technique for canceling or revocation of delegations in a similar way of certificate revocation in X.509
- We overcome the problems of saving the new keys related to proxy certificates in files without protection.

5.5. Disadvantages of the suggested solution:

- Limiting Delegating to one level of path: In our proposed method there is no cascade delegation. This means the delegated entity can not grant the delegation to other entity. Therefore the path of the delegation is limited to on certificate.

  This problem can be solved as a future work by using a similar field to that one already exists in the proxy certificate which expresses the maximum path lengths of Proxy Certificates.

  With assertion of finding a method to make the proxy annex on the all granted X.509 certificates be canceled in case of expiry of the validity period of the proxy annex related to the basic generated X.509 certificate (the first X.509 certificate granted proxy which is number one in the proxy path).
- Limiting the Dynamic Delegation to the X.509 owners: Each user who wants to grant a proxy of his rights and privileges (granted by proxy) or wanted to grant some right to him (the person enjoying the proxy) should hold a standard X.509 certificate.

5.6. The efficiency of our suggested solution (Modified Proxy Certificate Costs):

We measured the efficiency of our suggested solution at the level of users only (one level)

No cost for Key generation (one time, from X.509).

So the advantages of our solution become large when delegation is deep and frequent.

6. Conclusion

A rigid and secure authentication method is required for all e-services and application, During this paper, we covered the standard of Digital certificates (X.509 and proxy certificate), and its relation with dynamic delegation

Then we focused on the weaknesses of applying these standards to dynamic delegation and tried to come up with improved modified solution to make it applicable and more efficient to apply dynamic delegation to digital certificate standards.

this work is just a stone in the wall of greater solution which will take more time and effort to get higher security level and higher performance.

7. Future work:

Actually we have to apply our solution to reality, and measure the efficiency of our suggested solution for all levels involved in the system trying to prove our point of view.

References:

[1]. Butler, R., Engert, D. Foster, I., Kesselman, C., Tuecke, S., Volmer, J., and Welch, V., A National-Scale Authentication Infrastructure, IEEE Computer, 33(12):60-66, 2000.

[2]. Beiriger, J., Johnson, W., Bivens, H., Humphreys, S. and Rhea, R., Constructing the ASCI Grid. In Proc. 9th IEEE Symposium on High Performance Distributed Computing, 2000, IEEE Press.

[3]. CCITT Recommendation, X.509: The Directory – Authentication Framework. 1988.

[4]. FELICIA IONESCU, SILVIU POPESCU, Accessing Grid Resources from Portals and Applications, 9th WSEAS international conference on automation and information (ICAI'08), Bucharest, Romania, June 24-26, 2008.

[5]. Housley, R., Polk, W., Ford, W., and Solo, D., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, April 2002.

[6]. IETF Public-Key Infrastructure (X.509) (pkix) working group, January 2004 http://www.ietf.org/html.charters/pkix-charter.html,.

[7]. ITU-T Recommendation X.509,ISO/IEC 9594-8, Information Technology – Open Systems Interconnection- The Directory: Authentication Framework, 1997,1993,1988 Editions.

[8]. Li Xin and Mizuhito Ogawa, Proxy Certificate Trust List for Grid Computing, 2005 www.jaist.ac.jp/jinzai/Paper/JSSST05.pdf

[9]. Raghunathan, S. Mikler, A. R. Cozzolino, C., Secure agent computation: X.509 Proxy Certificates in a multi-lingual agent framework, JOURNAL OF SYSTEMS AND SOFTWARE, 2005, VOL 75; NUMBER 1-2, pages 125-137 , Elsevier Science B.V., Amsterdam.

[10]. Tuecke, S., Welch, V. Engert, D., Thompson, M., and Pearlman, L., Internet X.509 Public Key Infrastructure Proxy Certificate Profile, draft-ietf-pkix-proxy-10 (work in progress), IETF, 2003.

[11]. Von Welch, Ian Foster, Carl Kesselman, Olle Mulmo, Laura Pearlman, Steven Tuecke, Jarek Gawor, Sam Meder, Frank Siebenlist, X.509 Proxy Certificates for Dynamic Delegation, 2005

[12]. Xin, L. Mizuhito, O. A Lightweight Mutual Authentication Based on Proxy Certificate Trust List, LECTURE NOTES IN COMPUTER SCIENCE 2004, ISSU 3320, pages 628 632, SPRINGER-VERLAG.